Analisis Inisialisasi Proses Iterasi Fungsi Logistik Dalam Penentuan Bilangan Acak Terbaik

Claudio Basti Alfano[1],Alz Danny Wowor[2]

Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Jl. Diponegoro 52-60, Salatiga 50711, Indonesi
Email : 672012212@student.uksw.edu[1] , Alzdanny.Wowor@staff.uksw.edu[2]

Abstract

Rapid technological developments make the security of the data we send more vulnerable to attacks from outside parties in maintaining its confidentiality. One way to maintain confidentiality is that we can use cryptography, because cryptography can change the prefix data (plaintext) into processed data (chipertext) so that the data sent becomes safer. from this problem many cryptographic researchers make various forms of safer cryptosystems. This study examines cryptography using a 256-bit random number generator, using iteration equations of 4 types, namely a, b, c, d and has a key type 3 types and 3 types plaintext. This study also tested the key strength using runs up and down test, after that made data encryption using a combination of 3 types of keys and plaintext, so that in making the encryption chipertext will get the best and maximum randomness.

Keyword : cryptography, analysis, iterations, Best Random Numbers

Abstrak

Perkembangan teknologi yang pesat membuat keamanan data yang kita kirimkan semakin rentan terkena serangan dari pihak luar dalam menjaga kerahasiaannya. Salah satu cara untuk menjaga kerahasiaan tersebut kita dapat menggunakan kriptografi , karena kriptografi dapat mengubah data awalan(*plaintext*) kedalam data olahan(*chipertext*) sehingga data yang dikirimkan menjadi lebih aman . dari masalah ini banyak peneliti kriptografi membuat berbagai macam bentuk kriptosistem yang lebih aman.Penelitian ini meneliti tentang kriptografi menggunakan pembangkit bilangan acak 256 bit , dengan menggunakan persamaan iterasi 4 jenis yaitu a,b,c,d dan memiliki jenis kunci 3 jenis dan 3 jenis plaintext. Penelitian ini juga menguji kekuatan kunci menggunakan *runs up and down test* ,setelah itu membuat enkripsi data menggunakan kombinasi dari 3 jenis kunci dan *plaintext* tersebut , sehingga dalam membuat enkripsi *chipertext*nya akan mendapatkan keacakan paling baik dan maksimal.

Kata Kunci : kriptografi ,analisis, iterasi **,** Bilangan Acak Terbaik

---

[1]Mahasiswa Program studi Teknik Informatika Fakultas Teknologi Informasi Universitas Kristen Satya Wacana

[2]Staff pengajar Fakultas Teknologi Informasi Universitas Kristen Satya Wacana Salatiga